Carine Jackson

📍 Remote – Japan / U.S. | U.S. Work Authorized

✉️ carinejackson48@gmail.com | 🌐 GitHub • LinkedIn

English & Japanese (JLPT N2 – In Progress)

Professional Summary

Cybersecurity Analyst fluent in Japanese and English with hands-on experience in threat intelligence, vulnerability management, and security automation. Skilled in building CI/CD pipelines with integrated security tools (Semgrep, Bandit, Trivy), designing compliant cloud architectures (AWS, NIST, HIPAA), and conducting advanced threat research (APT34, MITRE ATT&CK, OSINT). Adept at Basic Python/Bash scripting, GitHub Actions automation, and vulnerability reporting. Strong communication skills and experience supporting global security teams.

Core Skills

- Threat Intelligence & Analysis: MITRE ATT&CK, OSINT (Shodan, VirusTotal, OTX), APT Profiling, YARA Rules, Wireshark, Nmap
- Security Automation & DevSecOps: CI/CD (GitHub Actions), Python, Bash, Regex, Automated Reporting, Docker/Kubernetes security scanning, Retire.js
- Vulnerability Management & Penetration Testing: Semgrep, Bandit, Trivy, Gitleaks, OWASP ZAP, Nessus, Burp Suite, Patch Management, manual penetration testing
- Cloud & Zero Trust Security: AWS (EC2, S3, IAM, MFA), VPNs, IDS/IPS (Snort), Zero Trust Architecture, containerized security, NIST/HIPAA Compliance
- Monitoring & Incident Response: SIEM (Splunk, ELK Stack), Risk Assessment, Forensic Readiness, Endpoint Detection & Response (CrowdStrike, SentinelOne), Incident Containment
- Governance, Risk & Compliance: NIST CSF, PCI-DSS, HIPAA, Security Policies & Procedures, Security Awareness, SQL, Tableau, Power BI

Projects & Experience (ATS Keyword Enhancements in Bold)

Cybersecurity Project Lead – AstroSkill LMS Connector | Coding Temple Tech Residency · Remote · 2025

- Developed a CI/CD security pipeline triggered by all Dependabot PRs and daily cron jobs, integrating Semgrep, Bandit, Gitleaks, Retire.js, and Trivy to ensure 100% coverage of 10+ monthly PRs, detect vulnerabilities within minutes, and maintain continuous compliance with NIST standards.

- Automated PDF/Markdown vulnerability reports using Python and GitHub Actions, embedding PR comments, security labels, and critical-issue auto-closure to reduce manual triage by ~40% and streamline remediation for a 5-developer team.

- Designed SOC-style incident workflows aligned with NIST CSF and SOAR-based automation practices, enabling auto-closing of critical PRs and flagging high-severity findings, cutting insecure code merges by 90% and accelerating incident resolution by 30%.

Cybersecurity Trainee | Coding Temple · Remote · Sept 2024 – Mar 2025

- Designed and deployed AWS-based secure network architecture with firewalls, IDS/IPS, VPNs, and continuous Nessus scanning, protecting 5 cloud services and reducing attack surface by 35% while ensuring NIST CSF compliance.

- Performed vulnerability assessments with Nessus, OWASP ZAP, and manual penetration testing, mitigating 20+ medium-to-critical risks in under 3 months through targeted OS and network hardening, preventing potential service downtime.

- Created and tested incident response plans and risk assessments aligned to NIST CSF, collaborating with cross-functional teams to improve SOC readiness and reduce MTTR in simulated incidents by 25%.

APT34 Threat Intelligence & Risk Assessment | Simulation · Remote · 2024

- Conducted research on APT34 using OSINT tools (Shodan, VirusTotal, OTX) and MITRE ATT&CK mapping, correlating 15+ TTPs with Wireshark data and Nmap/Burp Suite findings to produce actionable adversary profiles for SOC threat-hunting and endpoint detection & response (EDR) integration.

- Recommended proactive detection and mitigation strategies for 25+ IOCs, creating draft YARA rules and custom network signatures for SOC integration, increasing potential detection coverage of APT34 phishing domains and exploitation techniques by ~40%.

Cloud Security Strategy – HealthNet Simulation | Remote · 2024

- Built and validated a HIPAA-compliant AWS architecture with hardened EC2, encrypted S3, and enforced MFA, achieving 100% compliance in simulated audits and reducing data exposure risk in test scenarios by 45%.

- Authored forensic readiness playbooks and implemented phishing detection logic in Splunk SIEM and AWS GuardDuty, enabling SOC analysts to identify malicious emails and anomalies 30% faster in simulated incident drills.

Language Lore — Secure E-Commerce

- Designed and documented PCI-DSS–compliant network architecture securing payment processing for an e-commerce environment, implementing VLAN segmentation, WAF protection, and encrypted transactions to mitigate cardholder data theft risk.

- Conducted end-to-end vulnerability scanning with Nessus, OWASP ZAP, and Burp Suite, remediating all high-severity issues within 2 weeks and improving PCI compliance scan scores from 78% to 100%.

Education & Certifications

- Cybersecurity Certificate – Coding Temple, 2025

- Data Analytics Certificate – Break Into Tech, 2024

- CompTIA Security+ – In Progress

- B.A. Asian Studies & Political Science – Temple University Japan Campus